

1194.31 Functional performance criteria

1194.41 Information, documentation and support

(b) The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

(c) Alternatively, offerors may propose products and services that provide equivalent facilitation. Such offers will be considered to have met the provisions of the Access Board standards for the feature or components providing equivalent facilitation. If none of the offers that meet all applicable provisions of the standards could be accepted without imposing an undue burden on the agency or component, or if none of the offerors propose products or services that fully meet all of the applicable Access Board's provisions, those offerors whose products or services meet some of the applicable provisions will be considered eligible for award. Awards will not be made to an offeror meeting all or some of the applicable Access Board provisions if award would impose an undue burden upon the agency.

(d) Offerors must submit representation information concerning their products by completing the VPAT template at <http://www.Section508.gov>.

(End of clause)

[75 FR 10570, Mar. 8, 2010; 75 FR 14496, Mar. 26, 2010]

1352.239-72 Security requirements for information technology resources.

As prescribed in 48 CFR 1339.270(b), insert the following clause:

SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (APR 2010)

(a) *Applicability.* This clause is applicable to all contracts that require contractor electronic access to Department of Commerce sensitive non-national security or national security information contained in systems, or administrative control of systems by a contractor that process or store information that directly supports the mission of the Agency.

(b) *Definitions.* For purposes of this clause, the term "Sensitive" is defined by the guidance set forth in the Computer Security Act of 1987 (Pub. L. 100-235), including the following definition of the term:

(1) Sensitive information is " * * * any information, the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the,

conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

(2) For purposes of this clause, the term "National Security" is defined by the guidance set forth in:

(i) The DOC IT Security Program Policy and Minimum Implementation Standards, Section 4.3.

(ii) The DOC Security Manual, Chapter 18.

(iii) Executive Order 12958, as amended, Classified National Security Information. Classified or national security information is information that has been specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

(3) Information technology resources include, but are not limited to, hardware, application software, system software, and information (data). Information technology services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) The contractor shall be responsible for implementing sufficient Information Technology security, to reasonably prevent the compromise of DOC IT resources for all of the contractor's systems that are interconnected with a DOC network or DOC systems that are operated by the contractor.

(d) All contractor personnel performing under this contract and contractor equipment used to process or store DOC data, or to connect to DOC networks, must comply with the requirements contained in the DOC *Information Technology Management Handbook* (see DOC, Office of the Chief Information Officer Web site), or equivalent/more specific agency or operating unit counsel guidance as specified immediately hereafter [insert agency or operating unit counsel specific guidance, if applicable].

(e) Contractor personnel requiring a user account for access to systems operated by the contractor for DOC or interconnected to a DOC network to perform contract services shall be screened at an appropriate level in accordance with Commerce Acquisition Manual 1337.70, *Security Processing Requirements for Service Contracts*.

(f) Within 5 days after contract award, the contractor shall certify in writing to the COR that its employees, in performance of the contract, have completed initial IT security orientation training in DOC IT Security policies, procedures, computer ethics, and best practices, in accordance with *DOC IT*

Department of Commerce

1352.245-70

Security Program Policy, chapter 15, section 15.3. The COR will inform the contractor of any other available DOC training resources. Annually thereafter the contractor shall certify in writing to the COR that its employees, in performance of the contract, have completed annual refresher training as required by section 15.4 of the *DOC IT Security Program Policy*.

(g) Within 5 days of contract award, the contractor shall provide the COR with signed acknowledgement of the provisions as contained in Commerce Acquisition Regulation (CAR), 1352.209-72, *Restrictions Against Disclosures*.

(h) The contractor shall afford DOC, including the Office of Inspector General, access to the contractor's and subcontractor's facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DOC data or to the function of computer systems operated on behalf of DOC, and to preserve evidence of computer crime.

(i) For all contractor-owned systems for which performance of the contract requires interconnection with a DOC network on which DOC data will be stored or processed, the contractor shall provide, implement, and maintain a System Accreditation Package in accordance with the *DOC IT Security Program Policy*. Specifically, the contractor shall:

(1) Within 14 days after contract award, submit for DOC approval a System Certification Work Plan, including project management information (at a minimum the tasks, resources, and milestones) for the certification effort, in accordance with *DOC IT Security Program Policy* and [Insert agency or operating unit counsel specific guidance, if applicable]. The Certification Work Plan, approved by the COR, in consultation with the DOC IT Security Officer, or Agency/operating unit counsel IT Security Manager/Officer, shall be incorporated as part of the contract and used by the COR to monitor performance of certification activities by the contractor of the system that will process DOC data or connect to DOC networks. Failure to submit and receive approval of the Certification Work Plan may result in termination of the contract.

(2) Upon approval, follow the work plan schedule to complete system certification activities in accordance with *DOC IT Security*

Program Policy Section 6.2, and provide the COR with the completed System Security Plan and Certification Documentation Package portions of the System Accreditation Package for approval and system accreditation by an appointed DOC official.

(3) Upon receipt of the Security Assessment Report and Authorizing Official's written accreditation decision from the COR, maintain the approved level of system security as documented in the Security Accreditation Package, and assist the COR in annual assessments of control effectiveness in accordance with *DOC IT Security Program Policy*, Section 6.3.1.1.

(j) The contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

[75 FR 10570, Mar. 8, 2010; 75 FR 14496, Mar. 26, 2010]

1352.242-70 Postaward conference.

As prescribed in 48 CFR 1342.503-70, insert the following provision:

POSTAWARD CONFERENCE (APR 2010)

A postaward conference with the successful offeror may be required. If required, the Contracting Officer will contact the contractor within 10 days of contract award to arrange the conference.

(End of clause)

[75 FR 10570, Mar. 8, 2010; 75 FR 14496, Mar. 26, 2010]

1352.245-70 Government furnished property.

As prescribed in 48 CFR 1345.107-70, insert the following clause:

GOVERNMENT FURNISHED PROPERTY (APR 2010)

The Government will provide the following item(s) of Government property to the contractor. The contractor shall be accountable for, and have stewardship of, the property in the performance of this contract. This property shall be used and maintained by the contractor in accordance with provisions of the "Government Property" clause included in this contract.

Item No.	Description	Quantity	Delivery date	Property/Tag No. (if applicable)
.....